JUSTIFICATION
FOR AN EXCEPTION TO FAIR OPPORTUNITY

1. Contracting Activity: Department of Veterans Affairs (VA)
Office of Acquisition Operations
Technology Acquisition Center
23 Christopher Way
Eatontown, NJ 07724

2. Description of Action: The proposed action is for a firm-fixed-price delivery order issued under a National Aeronautics and Space Administration (NASA) Solutions for Enterprise-Wide Procurement (SEWP) V Government Wide Acquisition Contract (GWAC).

3. Description of the Supplies or Services: VA, Office of Information and Technology, Service Delivery and Engineering, Field Operations - National requires 21,000 SafeNet Universal Serial Bus (USB) eTokens for its Endpoint Administrators. This eToken hardware, combined with the SafeNet USB eToken authentication software previously acquired by VA, provides a secure means of two-factor authentication (2FA) of endpoint administrator higher level privileges to their endpoint workstation or laptop. Any unauthorized individual attempting to access the VA network as an administrator with associated higher level privileges would be denied as they couldn't complete required 2FA. The eTokens shall be delivered within 30 days of award and warranty support shall be provided for a period of 12 months upon Government acceptance of the eTokens.

4. Statutory Authority: The statutory authority permitting an exception to fair opportunity is Section 41 U.S.C. 4106(c)(2) as implemented by the Federal Acquisition Regulation (FAR) 16.505(b)(2)(i)(B), entitled "Only one awardee is capable of providing the supplies or services required at the level of quality required because the supplies or services ordered are unique or highly specialized."

5. Rationale Supporting Use of Authority Cited Above: Based on market research, as described in section 8 of this document, it was determined that limited competition is available for the required brand name SafeNet USB eTokens among resellers. VA's current authentication solution is completely comprised of SafeNet Authentication Manager software infrastructure, SafeNet MobilePASS One-Time Password licenses, SafeNet Luna hardware security modules, and SafeNet USB eTokens. This current infrastructure provides VA strong 2FA for server administrators, Citrix Access Gateway remote network access users, and endpoint administrators. Accordingly, only a SafeNet USB eToken can interoperate with the current infrastructure to provide the level of secured authentication of administrators and their designated privileges to the VA enterprise network. Use of any other vendors' eTokens would create compatibility issues as no other vendor has access to the proprietary source code of the existing SafeNet software required to ensure proper 2FA. Any other brand eToken would not authenticate the user, which would deny the user the required access to the end point and prevent the administrators and other remote network access users the ability to connect to their end point and perform their functions. This compatibility and interoperability issue would seriously impact the security of the enterprise network, and

introduce unacceptable risks to VA's network security posture, as well as inhibit Field Operations' administration responsibilities for monitoring that only authorized users and endpoints are accessing the network.

6. Efforts to Obtain Competition: Market research was conducted, details of which are in the market research section of this document. In accordance with FAR 5.301 and 16.505(b)(2)(ii)(D), the award notice for this action will be synopsized within 14 days of award on the Federal Business Opportunities Page along with a copy of this justification. In addition, this justification shall be posted to NASA SEWP V GWAC website with the solicitation.

7. Actions to Increase Competition: In order to remove or overcome barriers to competition in future acquisitions for this requirement, the Government will continue to perform market research to determine if there are any products and/or source providers available that will integrate with VA's current SafeNet infrastructure, or provide another 2FA solution that would enable future requirements to be competed.

8. Market Research: Market research was conducted by VA's technical experts in November 2015 by researching other eToken brands via the internet. Online research shows that Cisco is the only other vendor other than SafeNet that produces eTokens. While Cisco's eToken product offers similar functionality to the SafeNet USB eTokens, the Government's technical experts determined that Cisco's eToken could not meet the interoperability requirements with the VA's existing SafeNet software and infrastructure as stated in paragraph 5 of this justification. Access to SafeNet's proprietary 2FA technology is required for any other brand of eTokens to be interoperable with the SafeNet software currently in use as part of VA's 2FA infrastructure. As this proprietary technology can only be accessed through SafeNet USB eTokens, SafeNet USB eTokens are the only brand of eTokens that can meet all of VA's requirements.

Additional market research was conducted in February 2016 by utilizing the NASA SEWP V GWAC Provider Lookup Tool. It was determined that there were several NASA SEWP V GWAC holders that are authorized resellers of the required SafeNet eTokens such that competition is anticipated.

9. Other Facts: None.